Remarks

In the Non-Final Office Action dated June 21, 2010, claims 1 and 3-14 remain pending in this application; that the objection to claims 10-11 has been withdrawn; that the rejection to claim 4 under 35 U.S.C. §112, second paragraph has been withdrawn; that claim 9 stands rejected under 35 U.S.C. §112, second paragraph; and that claims 1 and 3-14 stand rejected under 35 U.S.C. §103.

By this response, applicants have amended claim 9 has been to correct an inadvertent error with respect to antecedent basis. No new matter has been added.

Rejection of Claim 9 under 35 U.S.C. §112

Claim 4 stands rejected under 35 U.S.C. §112, second paragraph, for lacking sufficient antecedent basis for the term "the number". According to the amendments to claim 9 shown above, this term has been changed to recite "a number". Amended claim 9 is clear, definite, and allowable under 35 U.S.C. §112. Withdrawal of this rejection is respectfully requested.

Cited Art

The following references have been cited and applied in the present Office Action: U.S. Patent Application Publication No. 2003/0221098 to Chen et al. (hereinafter referenced as "*Chen*"); and U.S. Patent Application Publication No. 2004/0081320 to Jordan et al. (hereinafter referenced as "*Jordan*"); U.S. Patent 7,293,289 to Loc et al. (hereinafter referenced as "*Loc*"); and U.S. Patent 6,118,869 to Kelem et al. (hereinafter referenced as "*Kelem*").

Rejection of Claims 1, 7-8, and 13 under 35 U.S.C. §103

Claims 1, 7-8, and 13 stand rejected under 35 U.S.C. §103 as being unpatentable over Chen in view of Jordan. Applicants traverse this rejection.

Claims 1 and 8 are independent claims. Claim 1 is a method claim, whereas claim 8 is an apparatus claim. Each of claims 1 and 8 recites substantially similar features which will be discussed below. For the sake of brevity of this response, the remarks below are intended to pertain to all the independent claims that include such similar features without further repetition of the remarks.

Chen fails to teach "setting a current encryption key and an old encryption key at an access point in the wireless network", as defined in the claims. Reference is properly made only to Chen herein because Jordan has not been applied against this feature in the claims. In paragraph [0055], Chen makes it very clear that he maintains "a memory 40 for recording the new ciphering key and all old ciphering keys". In other words, at the time that Chen generates and saves the new ciphering key K2 (or K3 or K4), the new key K2 (or K3 or K4) is already present in the memory that is apparently identified by the USPTO as corresponding to the old encryption key in the claims. Moreover, Chen fails to teach or suggest that any specific key held in memory 40 is an old key. There is no differentiation between any of the keys that are held in memory 40. Chen holds any keys preceding K1, as well all newly generated keys such as K2, K3, and K4, in memory 40 undifferentiated as to which is the old encryption key. All the keys in memory 40 are apparently treated as being the same.

Using the correspondences apparently set up by the examiner, Chen suffers from the same synchronization problems in the prior art – the same synchronization problems cured by Applicants' claimed invention. Based Chen's use of memory 40 as the storage medium for old keys and given the fact that the newly generated key K2 (or K3 or K4) is also present in that memory with all prior generated keys without any differentiation as to which one key is "the old encryption key" as defined in the claims, Chen would suffer an extended time of synchronization loss between the access point and the subscriber terminals because he would have to determine which key from all the keys stored in memory 40 is being used by the subscriber. Further, since Chen had already tested the newly generated key and determined that the newly generated key failed, Chen will turn to one or more of the encryption keys in memory 40 and duplicate that failed test again. This step constitutes duplication because the newly generated key that was tested in the failed test is also present in memory 40. Chen does not explain or suggest that such a result cannot occur. Chen does not even determine how he will roll back the encryption keys in

paragraph [0055] or elsewhere in his specification to find the actual (i.e., current) encryption key being used by the subscriber terminal. But since Chen does point to the storage in memory 40 for all keys including the most newly generated key, it is reasonable to conclude that Chen will duplicate the test using the most newly generated key again because he does not indicate that the keys in memory 40 are differentiated from each other in any meaningful way to avoid such a duplication.

Chen fails to teach, show, or suggest "resetting at the access point the current encryption key to equal the newly generated encryption key" and "resetting at the access point the old encryption key to equal an encryption key being used by a station in communication with the access point", as defined in the claims. Again, reference is made only to Chen herein because the examiner has not applied Jordan against these features in the claims. The analysis provided immediately above provides a good backdrop against which to further understand these differences between Chen and the claimed invention. When Chen generates the new encryption key (e.g., K2) in step 105, he maintains that new key separate and apart from the current encryption key (i.e., K1 in Chen's Figure 2). The key currently being used by the access point and the subscriber is stored in the storage location called K1 in Chen's Figure 2. At this point when the new key K2 is generated, the new encryption key apparently is placed in memory 40 upon generation. Recall that memory 40 has been identified as a repository for all the old encryption keys. Contrary to applicants' claimed features, Chen stores the newly generated key in the location for old encryption keys and Chen does not change the current encryption key (i.e., K1). To be complete, applicants note that Chen only replaces the current encryption key (i.e., K1) with the new encryption key (i.e., K2) at the very end of his process in "Finish" step 250. *See Chen at paragraph [0053].* Until the successful end of the process in step 250, Chen maintains the location K1 with the value of encryption key K1 and does <u>not</u> perform any updating of K1 with the new key K2. As a result, Chen does not reset the current encryption key and he does not reset the old encryption key in the manner required by each of the cited claim features.

As noted above, Chen does not differentiate between any of the keys stored in memory 40. But assuming arguendo that the last (i.e., most recent) entry into memory 40 of Chen is the "old encryption key"; Chen still fails to teach applicants' claimed features. The most

recent entry into memory 40 of Chen always constitutes the most recently generated encryption key, that is, K2. So continuing with the assumption, Chen resets the old encryption key in memory 40 to equal to the newly generated encryption key, K2. At the time that K2 is generated, K2 is not yet being used by the subscriber terminal or station communicating with the access point – K1 is the key being used by the subscriber and the access point. As a result, this assumption shows that Chen cannot conceivably teach or suggest "resetting at the access point the old encryption key to equal an encryption key being used by a station in communication with the access point", as defined in the claims. According to Chen's own teachings, K2 is the most recent addition to memory 40, which holds the old encryption keys, and K2 is not yet being used for communication by the station and the access point.

Contrary to the assertion by the examiner, Chen fails to teach or suggest "indicating at the access point a decryption failure for a data frame received from the station when the encryption key used by the station does not match the current encryption key", as defined in the claims. Reference is again made only to Chen herein because the examiner has not applied Jordan against this particular feature in the claims. Chen provides a test in step 240 of Figure 3 to see whether match after the subscriber has been supplied with the new encryption key, K2. While this step represents a determination, there is no express or implied teaching in Chen that "indicating" is performed by the step or the process at all. Chen does not indicate that the matching test for the challenge and confirmation texts failed. Instead, Chen merely decides to restart the process at step 110 or finish the process at 250. No indication of any kind is given by Chen.

Contrary to the assertion by the examiner, Chen fails to teach or suggest "resetting at the access point the old encryption key to equal the current encryption key when decryption using the new encryption key is successful", as defined in the claims. It should be noted that reference is again made only to Chen herein because the examiner has not applied Jordan against this particular feature in the claims. Chen accomplishes a successful decryption with the new encryption key K2 at steps 240 and 250 of his process. In paragraph [0053], Chen makes it clear that storage location K1 in Figure 2 is then updated to the new key K2 when the decryption is successful in steps 240 and 250. But, as already explained in detail above, Chen apparently stores K2 in memory 40 – that is, the location that holds all of Chen's old encryption keys – as

soon as K2 is generated in step 105. *See Chen at paragraph [0055].* There is no teaching or suggestion that Chen waits until decryption is successfully completed to store K2 in memory 40. There does not appear to be any condition precedent to the storage of K2 in memory 40.

Jordan fails to cure the defects discussed above with respect to the teachings of Chen. The examiner appears to hold this view since the examiner has not applied Jordan in combination with Chen against any of the features discussed above. For all the reasons set forth above, applicants maintain that the combination of Chen and Jordan fails to teach, show, or suggest all the features defined in independent claims 1 and 8 and the claims dependent thereon.

In light of all the remarks above, applicants submit that the features of independent claims 1 and 8 and the claims dependent thereon would not have been obvious to a person of ordinary skill in the art upon a reading of Chen and Jordan, either separately or in combination. Thus, it is believed that claims 1, 7-8, and 13 are allowable under 35 U.S.C. §103. Applicants request withdrawal of this rejection.

Rejection of Claims 3, 4, 9, and 14 under 35 U.S.C. §103

Claims 3, 4, 9, and 14 stand rejected under 35 U.S.C. §103 as being unpatentable over Chen and Jordan in view of Loc. Applicants traverse this rejection.

Claims 3-4 and 14 depend ultimately from independent base claim 1 and claim 9 depends from independent base claim 8. The dependent claims include all the features from their respective base independent claims and also include additional features over those presented in the base claims.

Applicants have already discussed the patentability of the base independent claims above will not repeat that discussion further, except to repeat that the combination of Chen and Jordan fails to teach, show, or suggest all the elements of the base independent claims. The examiner has cited Loc because the combination of Chen and Jordan failed to disclose the operation of an encryption failure counter, and conditions for incrementing the counter or resetting it to zero. Loc does not cure the deficiencies in the teachings of Chen and Jordan as described in the section above. Therefore, the combination of Chen, Jordan, and Loc fails to disclose or suggest all of the

elements of claims 3, 4, 9, and 14. Applicants request withdrawal of this rejection is respectfully requested.

Rejection of Claims 5-6 and 10-12 under 35 U.S.C. §103

Claims 5-6 and 10-12 stand rejected under 35 U.S.C. §103 as being unpatentable over Chen and Jordan in view of Kelem. Applicants respectfully traverse this rejection.

Claims 5 and 6 depend ultimately from independent base claim 1 and claims 10-12 depend from independent base claim 8. The cited dependent claims include all the features from their respective base independent claims and also include additional features over those presented in the base claims.

Applicants have discussed the patentability of the base independent claims already and will not repeat that discussion, except to repeat that the combination of Chen and Jordan fails to teach, show, or suggest all the elements of the base independent claims. The examiner has introduced Kelem because the combination of Chen and Jordan failed to disclose setting the encryption key to a null value. Kelem does not cure the deficiencies of Chen and Jordan as described for the independent claims in the sections above. Therefore, the combination of Chen, Jordan, and Kelem fails to disclose or suggest all of the elements of claims 5-6 and 10-12. Applicants request withdrawal of this rejection.

Conclusion

In view of the foregoing, applicants solicit entry of this amendment and allowance of the claims. If the Examiner cannot take such action, the Examiner should contact the applicant's attorney at (609) 734-6820 to arrange a mutually convenient date and time for a telephonic interview.

No fees are believed due with regard to this Amendment. Please charge any fee or credit any overpayment to Deposit Account No. **07-0832.**

Respectfully submitted,
Junbiao Zhang et al.

By: /Robert B. Levy/
Robert B. Levy
Attorney for Applicants
Reg. No. 28,234
Phone (609) 734-6820

Patent Operations
Thomson Licensing LLC
P.O. Box 5312
Princeton, New Jersey 08543-5312
November 19, 2010